Educational Games to Teach Fundamental Principles of Cybersecurity

Gregory B. White, Ph.D., The University of Texas at San Antonio; greg.white@utsa.edu
Johanna Jacob, Ph.D., Trinity University; jjacob1@trinity.edu
Natalie Sjelin, The University of Texas at San Antonio; natalie.sjelin@utsa.edu
Larry Sjelin, The University of Texas at San Antonio; larry.sjelin@utsa.edu

Abstract

The benefit of using serious games in education has been known for more than a decade (Dicerbo, 2012; Guillen-Nieto, 2015). Recently, the use of games to introduce cybersecurity principles to students in grades 5-12 has been conducted. Results have been very positive and the potential to replicate what was done in cybersecurity for other STEM disciplines has been proposed. This paper will address the use of the Cyber Threat Defender (CTD) Collectible Card Game to introduce cybersecurity principles to students. Of importance, especially to rural and Title I schools, is the use of the game along with lesson plans which have been developed to be used by teachers who have no background in cybersecurity. A second game, the Community Cybersecurity Game, was also briefly introduced as a companion that addresses a separate aspect of cybersecurity.

Keywords: Educational Games, Cybersecurity, Personal Development.

1. Introduction

Cybersecurity incidents have been increasing for several decades. This is a tremendous problem not just in the United States but globally. Estimates will vary but one source estimates that worldwide cybercrime costs will hit $10.5 trillion annually. (Fox, 2024) In 2024 the global average cost of a data breach according to IBM was $4.88 million. (Fox, 2024) All sectors are targets of cyberattacks from the financial industry to healthcare, government agencies, and manufacturing. Cybersecurity incidents are now considered one of the leading risks for organizations of any size. (Fox, 2024) Home users are not immune to attacks either with Bitdefender, a home security solution, reporting an average of 10 attacks on connected devices in the home every 24 hours.

To address the cybersecurity problem, many colleges and universities have developed cybersecurity programs awarding degrees or concentrations in cybersecurity. Unfortunately, the demand far exceeds the availability with currently 514,319 open cybersecurity positions in the U.S. alone. (Cyberseek, 2025) The degrees and concentrations, along with professional certifications, are an attempt to address this ever-increasing number of open, unfilled positions but doesn't directly address the additional issue of cybersecurity in the home.

Cybersecurity is a topic that every employee needs to know something about. In the U.S., some professionals have proposed the way to accomplish a broader, national cybersecurity awareness program would be to introduce cybersecurity principles to students in grades K-12 with age-appropriate lessons being developed. Some states have moved to try and establish a minimal requirement to have students learn principles of cybersecurity, but this effort is sporadic and heavily dependent upon the individual states. A 2020 study of the state of cybersecurity education in K-12 schools did not paint an encouraging picture, especially in small (rural) and high-poverty school districts:

> *Students in small and high-poverty districts are significantly less likely to be exposed to cybersecurity education, as are those attending public versus private schools, or living in communities with no cybersecurity companies. These results suggest that relatively more privileged students may have more opportunities to be exposed to the field. This lack of access can have consequences down the road as coursework can build interest in careers*. (Cyber.org, 2020)

One way to reach these underserved populations could be through the use of educational gaming. It is well known that especially with the current tech-savvy generation, gaming presents a number of benefits such as improving computer and digital literacy, enhancing social and soft skills, improving problem solving skills, and promoting motivation; (Learning Lands, 2025) Of special significance to this paper is the fact that educational gaming in a topic such as cybersecurity can provide an introduction to a topic that teachers are not familiar with or comfortable with introducing to their students if they have to create lessons on their own.

URI: https://hdl.handle.net/10125/112258
978-0-9981331-9-5
(CC BY-NC-ND 4.0)

2. Lack of Teachers

The need for more cybersecurity professionals has driven a push to provide cybersecurity training and classes in colleges and universities. There are hundreds of programs now recognized by the Department of Homeland Security (DHS) and the National Security Agency (NSA) as Centers of Academic Excellence in Cybersecurity. More recently some states and several universities have pushed for cybersecurity training to extend to high schools and middle schools. The CyberPatriot program, a cybersecurity competition for middle and high schools, is managed by the Air and Space Force Association. This program has run for over a decade and in 2025 had over 5000 teams participate in the program in the United States. With this many teams, it might be assumed that there was a broad cross section of schools participating from across the country with a corresponding number of schools teaching cybersecurity courses. Research has shown, however, that this is not the case.

In her 2024 dissertation, Dr. Johanna Jacob reported that a 2023 survey on the availability of cybersecurity education in public high schools indicated that only 3.6% of high school students had access to cybersecurity courses. The survey drew data from 11 states that represent 44% of public high schools in the nation. This amounts to 6400 public schools and education centers. (Jacob, 2024) Dr. Jacob conducted her own study of the CyberPatriot competition to determine the penetration of cybersecurity in schools. She was particularly interested in rural and Title I schools having noticed what another 2020 survey referred to as "cyber deserts"

> *Cybersecurity deserts are zones where there is a significant disparity of access to programs and opportunities according to the socio-economic status of the intended population. This skill gap poses serious implications for adopting informed and knowledgeable cybersafe practices.* (Cyber.org, 2020)

Dr. Jacob's research involved an examination of the teams that participated in the CyberPatriot competition to determine the representation of Title I schools. Her results were concerning.

> *States with densely populated rural student population and high participation in CyberPatriot had no representation from Title I schools. For instance, New York and New Jersey together make up 17 percent of the rural student population and peaked in numbers among the Northeastern states with more than 170 teams. However, not one team represented a Title I school or school district. States such as Maine, Vermont, South Dakota, North Dakota, Mississippi, New Hampshire, and Iowa, which have sizeable rural student numbers and Title I schools, are underrepresented significantly. States with lower educational outcomes and with rural schools placed in poor communities are invisible and underrepresented largely. Mississippi, West Virginia, and Alabama have a sizeable rural student population with half of the state's students enrolled in rural districts that have large enrollment, but their participation did not include any Title I schools.* (Jacob, 2024)

A chief reason for non-participation of schools is the lack of a teacher with the background to introduce cybersecurity to students. This is true of not only cybersecurity, which can be considered somewhat of a specialty in STEM, but more general STEM disciplines as well. Dr. Jacob found that only 7% of the teachers in Title I schools who responded felt that their school provided avenues for STEM education while 30% of non-Title I schools felt theirs did. (Jacob, 2024) Without teachers who have a background in the various STEM disciplines, and the specialty disciplines such as cybersecurity, it is unrealistic to expect a strong penetration of STEM in schools. This is especially true for Title I and rural schools. If this disparity and the nation's need for more STEM professionals is to be addressed, we must reach students in K-12 to introduce them to the disciplines early and we need to provide a way for teachers in these schools to be able to introduce the topics without requiring a strong background in the various disciplines. This is where gaming can help to make a significant contribution.

3. Experiential Learning

Good educational games should be fun and should motivate the players to learn about the domain the game addresses. (Nachimuthu, 2011) In their study, Sandford et al. determined that both teachers and students found using games in lessons was motivating and that:

> *for the game to be of benefit to teachers, it need only be accurate to a certain degree: there may be wider inaccuracies within the game model, but these do not necessarily preclude the game from being used meaningfully in a lesson.* (Sandford, 2006)

The finding of games being motivational is not surprising today with numerous examples of games being used in education. However, the statement

concerning the accuracy of the game not being as critical as some might think is significant for teaching cybersecurity in middle and high schools where a lack of teachers with a cybersecurity background and a lack of cyber resources exists. Another factor that has been shown to be useful in a student's ability to understand various topics is experiential learning. Experiential learning is focused on learning through experience where a student can learn while "Doing, Reflecting, Thinking and Applying". (Kong, 2021) Students that can take part in a tangible experience are more likely to be able to apply what they have learned in real-world circumstances. The problem with doing this for cybersecurity in middle and high schools is, as previously mentioned, the lack of knowledgeable students and computing resources to provide hands-on experiences. We believe that a well-structured educational game can assist with both limitations. We designed two cybersecurity games that introduce real-world situations in cybersecurity that provide students with experience in dealing with real challenges in cybersecurity. While the students will not learn how to configure a firewall or intrusion detection system, they do experience how these two security tools help them defend their computer systems and networks.

4. Cyber Threat Defender

Cyber Threat Defender (CTD) is a collectible card game developed in 2016 by the Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio. It was designed as a way to interest students in cybersecurity and to teach basic cybersecurity principles. When it was designed, the emphasis was on developing a fun game that individuals would enjoy playing and want to play again. The game was designed to NOT require any knowledge of cybersecurity in order to play the game. The secondary emphasis when designing the game was that by playing the game, individuals would gain an understanding of basic cybersecurity principles. Fun first, education second. Too often these two elements are flipped but if the game is not fun, individuals won't continue playing and the learning will cease. The game was envisioned to be playable by individuals from "11 to 99". As such, middle and high school students could play the game with friends and family members and the lessons learned through playing the game would occur for more than just the students themselves. Figure 1 shows an image of a CTD tournament held in San Antonio, TX open to anybody from age 11 up.

Figure 1. Cyber Threat Defender Tournament.

The card game is similar to other collectible card games in that the basic set of rules are very short with the description of what each card represents and the rules governing the card contained on the card itself. There are four types of cards in the game. Asset cards consist of various devices that can be used to increase the size of your network with the goal of creating as large a network as possible. Players receive points for the devices they have in play such as a laptop computer or a computer server. Attack cards represent attacks on their opponents' cards. These cards include common cyberattacks that occur on a regular basis such as an attack via malware or attempting to crack a user's password. Players lose points from attacks on their assets. Defense cards are used to protect various aspects of a player's network such as updating or patching operating systems and security devices such as firewalls. The final type of card is an event card which can be either beneficial or detrimental depending on the specific card. These cards represent events that can occur such as a power outage, hardware failure, or employees attending security training. Figure 2 shows an example of an attack and a defense card.

Figure 2. Sample CTD Game Cards.

As shown in Figure 2, each card provides a description of what the card represents followed by a short description of how this card is used in the game. Just below the image is listed the category the card falls

into. In this case "Attack – Malware" and "Defense – Software" At the top of the card is the name of the card and to the far right is a small box with a number in it. This box shows the value of the card if it is a resource or, as is the case of the attack card shown in Figure 2, it is the number of points that the opponent loses while the card is in play. Notice that the "Anti-Malware/Virus" defense card states it will remove any Attack-Malware category cards that are in play attacking the player. This is one example of the learning aspect of the game. There are combinations of cards that go together. An attack card has a corresponding defense card. This synergistic relationship between cards helps the students learn what attacks that can affect their systems but also what they can do to defend against the attacks.

The game is easy to learn and to play and lasts about 15 minutes. Each player starts with seven cards in their hand, a desktop computer and an ISP connection in front of them (to start their network) and no points. The winner is the first player to reach an agreed upon total, usually 30 points by expanding and defending their network. Each round a player can play up to three cards during their turn. This doesn't include event cards which can be played at any time with no limit to the number that can be played. As mentioned, the players do not need to know anything about cybersecurity to play the game – everything they need to know is on the cards. Playing the game will introduce players to, and provide experience with, elements of cybersecurity needed to defend their systems. In the case of the cards shown in Figure 2, the players will learn that a Trojan Horse is a type of malicious software that is hidden in another program. They will learn that another name for malicious software is malware, and they will experience defending their systems with anti-malware software. Figure 3 shows another example of a pair of related cards with a different lesson to be learned. In this case the importance of encrypting their wireless networks otherwise an attacker can listen to communication on the network. While the game is designed to accurately represent the real-world cybersecurity field, some allowance has been taken to make the game more playable. Home wireless routers will generally come utilizing encryption so this may not apply to a home network. However, accessing an open wireless network in a public location may expose them to "wireless sniffing" where an attacker can listen to their traffic.

The CTD starter deck contains a number of these card combinations. If there is an attack card, there is an event or defense card that will counteract the attack. By providing these combinations players will be exposed to basic elements of cybersecurity. The collectible card game genre is a perfect fit for an educational game such as CTD. Individuals who have played a collectible card game will be used to the idea of learning what each card

Figure 3. Wireless Sniffing and Encryption.

does by studying the cards. For games such as Magic the Gathering or Pokémon, players will need to know what each creature's attack and defense elements are and to understand when they can be used. To be competitive, players have to study their cards to develop their strategy for playing the game. For an educational game such as CTD this means the players by studying the cards will learn about elements of cybersecurity in order to be prepared to play, and win, the game.

Another element of collectible card games are the booster packs that can be purchased to expand a starter deck. For some games the starter deck will be the same but for others there is an element of randomness to what cards the player starts with. To the starter deck, players will add or swap out new cards they may obtain through booster packs. CTD has incorporated the concept of booster packs with one exception – all of the cards in a booster pack are the same for each booster release. This means there is no randomness in terms of the cards a player receives. The result is that the onus is on the player to develop the best deck they can based on the strategy they elect to employ. Do they want to be more offensive, defensive, or have an equal amount of attack and defense cards? Whatever they decide, they need to understand the advantages and disadvantages for each card to develop a "winning" deck. They need to study the rules on each new card and will be introduced to other elements of cybersecurity as they do so.

The main reason the boosters in CTD are designed the way they are is each booster release is intended to introduce a new element of cybersecurity to the players. The boosters provide teachers a way to introduce new elements to students in their class. There are a number of existing boosters. The first booster pack was the CyberPatriot Booster. It included a few cards that were already introduced in the starter deck (in case a player wanted to add more copies of one of them to their playing deck) but also introduced a number of new cards such as Spear Phishing, Data Exfiltration, Ransomware, and a CyberPatriot card. CyberPatriot is a middle and high school cybersecurity competition. The pack was

intended to make more students and teachers aware of this competition. The CyberPatriot card eliminates "Phishing", "Password Cracked", and "Forgot to Patch OS" cards. The reason behind this is these are elements students who participate in CyberPatriot will know to look for and know how to defend against. A teacher could use this booster to introduce both the CyberPatriot competition as well as the additional new elements of cybersecurity presented in the new attack cards.

Another example of a booster pack is the Advanced Threat Booster. This is a particularly interesting one as it includes 11 new attack cards and one new defense. The defense card is the "Intrusion Prevention" card which introduces the concept of an intrusion detection system which is a major type of defensive system used in networks. The attacks include "Rogue Employee", "Drive-by-Download", and "Footprinting". Again, all of these cards provide a teacher the opportunity to introduce new concepts in cybersecurity to students. Figure 4 shows two of the cards in this booster pack.

CTD was designed to be provided to schools and school districts for free. Sponsorships have been provided that allowed the CIAS to produce and send decks of cards to schools and school districts throughout the nation and several countries. Sponsors have paid for special booster packs which can include a particular emphasis the sponsor wants to promote. While over 92,000- decks have been shipped to schools since 2016, the number who want decks to be provided exceeds the funding obtained from sponsors. Schools can request to be placed on a waitlist to have decks provided to them when sponsorships are obtained, or they can actually purchase them from the CIAS directly. Another option which has been provided is to download an electronic version of the game from the CIAS website. This version allows students to play against the computer. They can set up their own deck to test different strategies and can have the computer utilize different strategies as well. The game can be downloaded along with several other short security-related games, all of which are free. These can be found at (CIAS, 2025).

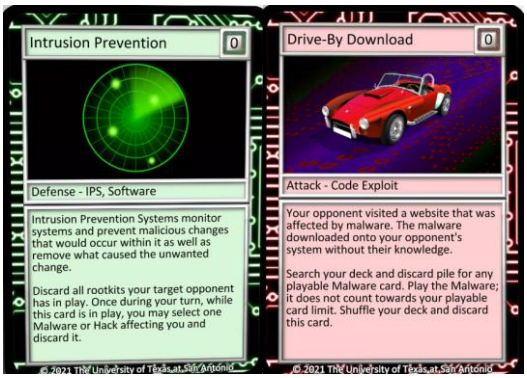

Figure 4. Cards from the Advanced Threat Booster.

5. Impact on Rural and Title I Schools

In an effort to assist teachers in the classroom, lesson plans were developed that could be used by teachers to introduce both the game as well as the cybersecurity concepts introduced in the game. The lesson plans were developed to be useable by teachers who did not have any background in security, but elements of each plan could also assist those who might have been introduced to cybersecurity at some point. Each lesson plan included a discussion of the different card pairings to provide additional background on the concept the card combination introduced. The lesson plan also included links to additional resources and possible activities the teacher could use to further illustrate the security concept. The recommendation was for the teacher to provide the card game to the students, let them play it for a while such as during a class period when the class had a 20-minute block that was free, and then after the students had played the game to use the lesson plans to drive home the concepts. The idea was to introduce the concept by saying something along the lines of "remember when you played the game how these two cards worked?" and then expanding on the security concept. As an example, the "Password Cracked" and "Security Training" combination could be used to generate a discussion of passwords and what makes a password a "good" password and how you can ensure you have selected a good password. As an activity, the teacher could introduce one of the available online password checkers and allow students to suggest a password which could then be checked for strength and for how long it might take to crack. For an example site, see (Bitwarden, 2025). This site also has additional information on passwords the teacher could use. It should be pointed out that the concepts and the level of detail to be able to discuss them is not so deep that the teacher will need to have a background in cybersecurity. The password example is a good one to illustrate this point. The concept is fairly simple, and the activity will drive home the point. At this point the teacher could conclude the lesson or could delve deeper if desired. A more intensive discussion of passwords might include a discussion on the length of the password versus the number of allowable characters that can be used in the password. This might be of interest to more advanced students but would not be required to illustrate the basic concept from the game.

Dr. Jacob reported in her dissertation of an experiment in conjunction with Angelo State University and the Eden, TX School District to utilize a cybersecurity card game in conjunction with lesson plans developed for teachers. Five specific topics in cybersecurity were explored in these lessons and with the cards. These included passwords, phishing,

backups, Wi-Fi security, and digital foot printing. In addition, a lesson on cyberbullying, which had no associated cards in CTD, was also provided. (Jacob, 2024) Results showed significant promise for this approach to be successfully implemented. Examining the lesson on passwords as an example, post-test results indicated a significant improvement in an understanding of effective password selection with 82% of students now selecting complex passwords. (Jacob, 2024) Student responses were positive from the experiment. A sampling of just a few student responses are as follows: (Jacob, 2012)

> *"Cybersecurity is important to know and I think I have learned enough to know how to use the basic skills to protect myself"*
>
> *"It was fun and my passwords are now more secure"*
>
> *"I learnt to make good passwords and use a tool to see how long it takes to break my password"*
>
> *"Cybersecurity is important and helpful in today's day and age. I am glad to know the basics of this field, even if it's not a good job for me"*

6. Community Cybersecurity Simulation

CTD provides an introduction to various technical aspects of cybersecurity. This is an important part of the discipline, but it does not address a major reality that organizations face. CTD does not introduce the challenge of determining how to spend a limited cybersecurity budget. Organizations do not have an unlimited budget and face the real challenge of determining where to spend their limited funding. Security managers have to decide what is most important to their organization and their clients and what threats they face that can impact what is referred to as their *Business Essential Functions* or, for government organizations, their *Mission Essential Functions*.

> *Business budgeting tendencies show that cybersecurity investments receive only a small part of the allocated IT budget. Cybersecurity funds must be distributed wisely to ensure valuable outcomes, prove the chosen security direction effective and minimize resources' waste.*
>
> *The main challenge is how to achieve effective security spending. How much should businesses allocate to cybersecurity, and what factors like company size or maturity does it depend on?* (Srėbaliūtė, 2024)

A separate game was developed to help individuals examine this aspect of cybersecurity. It has been used and has helped individuals in organizations better understand this challenge. This game, or simulation, is equally useable by teachers in middle and high schools to introduce this separate aspect of cybersecurity which complements the lessons they learn playing CTD.

The origin of this simulation was the 2020 National Level Exercise (NLE 2020). According to DHS/FEMA:

> *The National Level Exercise (NLE) is the nation's cornerstone exercise for validating progress toward promoting and sustaining a prepared nation to respond to catastrophic events.*
> *The four-year National Exercise Program cycle includes two operations-based national level exercises.*
> *The NLE is an opportunity for all levels of government, the private sector, nongovernmental organizations, and community groups to test operational capabilities, evaluate policies and plans, familiarize personnel with roles and responsibilities, and foster meaningful interaction and communication across the nation. Scenarios for the NLE range from natural disasters to man-made attacks and address the specific types of threats and hazards that pose the greatest risk to the nation.* (DHS/FEMA, 2025a)

NLE 2020 was designed "to examine and validate the Nation's prevention, protection, and response capabilities during a multidimensional threat that included widespread cyber-attacks which led to significant impacts on critical infrastructure and community lifelines." (DOD/FEMA, 2025b) While the major portion of the exercise was eventually canceled due to COVID-19, a number of activities had occurred to help the intended participants prepare for the exercise. These activities included cybersecurity workshops and the Cyber Ready Community Game which is sometimes referred to as a simulation instead. The CIAS was contracted by DHS to develop an "engaging strategy board game to explore the dynamics of cyber preparedness. Using gameboards and playing cards, players group within the game "community" to decide how to invest cyber credits to protect essential services." (DHS/FEMA, 2025c) The gameboard is still available from DHS/FEMA though they are currently out of stock. Figure 5 shows a group of individuals playing the game.

Figure 5. Professionals Playing Cyber Ready.

Cyber Ready was designed to be used in preparation for a national level exercise. It included a strong focus on emergency management during a cybersecurity attack. The game was modified by the CIAS to solely focus on cybersecurity and Mission Essential Functions (MEF). It is designed to introduce the core functions of the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF). The CSF describes six functions considered essential in the development of a cybersecurity program: Govern, Identify, Protect, Detect, Respond, and Recover. (NIST, 2024) The game addresses three elements of cybersecurity: 1) The challenge of planning and allocating a limited budget to protect an organization's assets; 2) The need to cover as much of the six core functions as the budget allows; and 3) Introduce cascading effects which occur when one sector experiences a failure which impacts other sectors as well. An example of the Cyber Ready game board can be seen in Figure 5. The current board is divided along the NIST CSF core functions with each function represented in a column. Each column presents potential security controls – mechanisms that can be purchased to create the organization's approach to security. There are 24 security controls but the budget provided is not sufficient to purchase them all. They will have to make tough decisions about which controls to purchase.

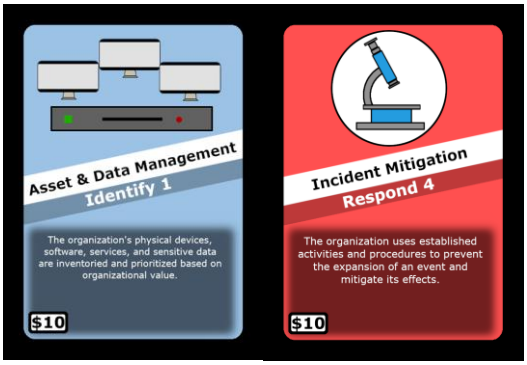

Figure 6. Example of Potential Security Controls

Figure 6 provides two examples of security controls players may choose to fund. Each control purchased will be placed on the board covering its location. The cards show which core function the control fits into, in this case Identify and Respond. The card also provides a brief description of what the control entails and also shows the cost in the game for the control.

In order to emphasize the importance of maintaining essential community functions, each board lists four Mission Essential Functions. These are critical services needed daily for the community to function effectively. Not only are they essential for the organization represented by the board, but they may also be essential to other community sectors. Two MEFs for the city government board are shown in Figure 7.

Figure 7. MEFs 3 & 4 for the City Government

The game is played in two phases. The first phase consists of the teams determining how they want to spend their budgets. They have an insufficient budget to defend against all possibilities, which is indicative of what organizations actually experience. Six different team boards can be used, each representing a different sector. The sectors, each with their own MEFs, are:

- City Government
- City Utilities
- Community Bank
- Community Hospital
- K-12 School District
- Private Sector Business

After the teams have made their selection of security controls, the game proceeds to its second phase. In this phase security events will occur which the players then determine if their selections would address. An inject card is turned over for each team to address. The cards can be shuffled and will thus be random, or the organizer of the event can choose specific injects for each team's turn if specific lessons are to be covered. Two inject cards are shown in Figure 8 to illustrate the type of events that are represented on the injects. The first example is for an inject that will only impact the team that received the inject. The second is a bit more involved in that it includes an impact on an MEF that

will have broader impacts across the community. The format of both is similar. On the left and right side of the cards are a character and number combination. Each points to a specific security control that is represented on the game board. If that space is covered by a security control card, in other words, if the team has elected to purchase that security control, then the attack is considered to be at least partially contained. If both security controls are covered then the card has no impact on the team. If either is not covered, then the team loses points. The card includes a description of what the inject entails to explain to the team what has occurred and so they can see how the controls they selected either did or did not address the event. The second card shown in Figure 8 has an additional section. Just above the event description is shown "MEF Water". An entry in this section of the card indicates that one of the MEFs for the team has been impacted. The description will then explain what the impact is to the organization with the loss of the MEF and may additionally state that other sectors in the community may also lose points because of a cascading impact across the community. In this case, the community's water system has been impacted, which in turn impacts the rest of the community.

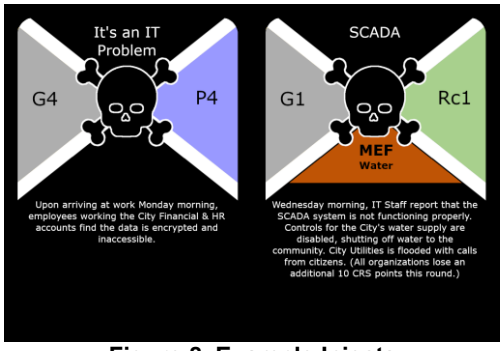

Figure 8, Example Injects

Cyber Ready has been played by community leaders across the country. The new, more cyber focused version has also been played by community leaders as well as students in college and high school classes. The budget challenge is often not addressed in cybersecurity courses in college and the experience of instructors and their students who have used the game has been very positive. It helps students to visualize one aspect of what they can expect when they enter the security field. The game was also introduced as a companion to the CTD game in a small, rural high school to determine 1) how well the students grasped this different aspect of security; 2) Whether they understand the importance of planning for Mission Essential Functions and the possibility of cascading impacts across the community when an MEF for a certain organization or sector was impacted; and 3) Whether the two games complemented each other in that they introduced different elements of cybersecurity. The students were first introduced to CTD and had an opportunity to play it during two lessons. Card combinations were then pointed out to the students and were discussed as previously described. Then another lesson was devoted to the Community Cybersecurity Game. Pre- and post-tests were administered and showed that the students had learned the basic security principles illustrated with the different card combinations in CTD and that they understood the challenge of budgeting for cybersecurity and the importance of protecting an organization's mission essential functions. Figure 9 is a picture of students in the rural community high school playing the community game.

Figure 9, HS students play Community Game

7. Effectiveness of the Games

Table 1. provides a high-level synopsis of what each game is focused on an the desired outcome of the game. We believe the outcomes have been realized. CTD has been played by over 400,000 students since 2016. In a 2024 survey of the CTD computer game that received 625 responses, over 75% reported a favorable or highly favorable opinion of the game with less than 7% responding unfavorably. The rest were neutral. Eighty-five percent said that they would recommend the game to their friends. Very satisfyingly 77% said they felt their knowledge of cybersecurity had improved as a result of playing the game with 52% reporting that as a result of the game they had modified their behavior based on what they had learned in the game. Also of

	Main Focus	Desired Outcome
CTD	Cyber Attacks and Defenses	Know common attacks and understand how to defend against them; Understand specific cybersecurity consept
Community Budget Game	NIST CSF; Cybersecurity Budgeting	Knowledge of the six CSF core functions; understand budgeting constraints and challenges

Table 1. Focus and Desired Outcome for the Games

importance, 80% said that playing the game had increased their interest in pursuing a possible security career. The survey was taken by individuals who played the game and were in grades 5-12 or were in college.

In an earlier 2024 survey of educators using one of the three cybersecurity card games developed by the CIAS, 210 responses were received from teachers in grades K-12. Of these, 135 teachers reported using CTD in their classes. Of these teachers, 75% stated they found the game extremely or very helpful, 23 % stated it was somewhat helpful, and only 1.5% stated "it was not so helpful" or "not at all helpful". Of the 2 teachers providing a negative response, one left no comment explaining why the negative response was given. The other, who had only used the game for a "year or less" said that it required "too much of a learning curve for students unfamiliar with the card game 'magic.'" No further details were provided, and it is unknown whether the students in the classes of those who valued the game had a background with "Magic, The Gathering" or not.

Many very positive comments have been received from teachers who utilized CTD. A few are mentioned here as a sample.

> *My students love this game. We held a class tournament last month and will have our final tournament next month. I have students who are not in my class come to me at lunch and ask for packs of cards to play with their friends*. – North Carolina High School Teacher

> *"I've used Cyber Threat Defender for three years in a row now, and it is a great way to engage my high school students! They like the gaming interaction, and it helps shape their cybersecurity related thinking while sneaking in some educational concepts."* – Tennessee High School Teacher

> *"My students love playing Cyber Threat Defender. We use it in my computer repair course, and it is really the only exposure to security they get. I find that as they continue to play the game and get used to the available cards, they are also getting a basic understanding of the different threats and security features that are out there."* – Computer Science High School Teacher

> *"This is a really great investment and a great way to bring kids into the world of cyber."* – Texas Middle School Teacher

The community cybersecurity simulation/game has been used in college courses and with one rural high school class. No survey has been conducted at this point to measure the level of acceptance of this separate game and its benefit in teaching cybersecurity. Only anecdotal evidence received from the faculty who have used it exists currently. Those who have used it feel that it does provide a different, and important, perspective on cybersecurity that complements other lessons and CTD. Further research is needed in this area.

8. Potential for Other Stem Disciplines

The success in using games to teach basic principles of cybersecurity was experienced in the several schools where the games were used. Not only was there a visible increase in the understanding of cybersecurity principles by the students but they were also introduced to the potential field as a career opportunity. This is especially important for rural and Title I schools where the understanding of the field was less prevalent before participating in the games. This same lack of exposure also exists for other Science, Technology, Engineering, and Math (STEM) fields. The same challenge exists in that few teachers, especially in rural and Title I schools, have a background in the various STEM disciplines. It is not uncommon for teachers to not have any background in the discipline they are asked to teach. For example, the teacher in the rural school in which the Community Cybersecurity game was played is a history teacher who volunteered to teach programming despite not having a background in computer science.

If developing a game for a STEM discipline it is important to keep in mind the three concerns previously mentioned: 1) the game has to be fun; 2) the players should not require previous knowledge of the subject; and 3) the students should be able to pick up basic principles related to the subject simply by playing the game. In order to satisfy the first concern, the game needs to be challenging and can be played multiple times while maintaining the students' interest. CTD is not the only card game related to cybersecurity, but it is the only one in the authors' experience that has gained the following of students and teachers alike. The main reason for this is because it can be played repeatedly and is fun to play. The developers attribute this to two factors. The first is that there is an obvious competitive aspect to the game with attacks and defenses and a definite winner in each game. In order to win the player has to create a "winning deck" which provides a challenge for the student. The second aspect to the game that makes it fun is the random nature of each game. This is similar to every card game in which the deck is shuffled before playing. This means if students play multiple games, they will experience a different sequence of cards played with potentially a different outcome each time they play.

An example of a possible card game that could be created to help introduce another STEM discipline might be space exploration. An objective might be for each player to build a space program with the capability to successfully send and return astronauts to Mars. While the game might not have "attack" cards that impact an opponent the way they do in CTD, there are a number of issues that can go wrong that would prevent the success of certain advances in a player's attempt to send a crew to Mars. Many actual examples have occurred previously in NASA's space program which could be modified so they are realistic but do not point to any actual event that resulted in the loss of life. "Defending" against these "attacks" would be various technical solutions to problems associated with space exploration. These cards would make the game challenging for players, and the game will be "replayable" without the outcome foreordained. In a similar manner, the field of medical science could provide another rich area for a game that would introduce the field and possible careers to students who might otherwise not learn about the field. The authors hope to explore these possibilities in the future.

9. Conclusion

The most significant lesson learned from the research into using games to teach cybersecurity principles is that they are absolutely beneficial. Even more significantly, the fact that the game can introduce basic lessons in cybersecurity without the teacher needing a background in cybersecurity is of paramount importance. Since research has shown that rural and Title I schools lack cybersecurity savvy teachers, being able to use a game to introduce concepts and provide a basic experience is significant. With the global lack of cybersecurity professionals, and the need to secure our cyber assets from home networks to critical infrastructures, it is important that we introduce students in K-12 to age-appropriate cybersecurity principles. Especially important to rural and Title I schools is the ability for games to introduce students to possible career fields they otherwise would not be exposed to.

Research into and development of additional resources that can build upon the success of CTD and the Community Cybersecurity Game is needed to further encourage students to consider a career in this field. Even for students who are not interested in cybersecurity as a career choice, exposure to cybersecurity principles will help them in whatever career they choose as computers permeate society.

A final area of potential research is to examine whether the success of the CTD game can be replicated for other STEM disciplines. This could include card or electronic versions. The same problem exists in rural and Title I schools for other STEM disciplines and methods to introduce STEM fields needs to be explored.

10. References

Bendovschi, Andreea (2015), "Cyber-Attacks – Trends, Patterns and Security Countermeasures", 7th International Conference on Financial Criminology, April 2015, Waldham College, Oxford, United Kingdom.

Bitwarden (2025), "How Strong is your Password?", https://bitwarden.com/password-strength/

CIAS (2025), "K-12 Cybersecurity Games", Game Launcher, https://cias.utsa.edu/k-12/cybersecurity-games/

Cyber.org (2020), "The State of Cybersecurity Education in K-12 Shools", https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf

Cyberseek.org (2025), "Cybersecurity Supply/Demand Heat Map", https://www.cyberseek.org/heatmap.html.

Dicerbo, Kristen (2015), "Taking Serious Games Seriously in Education", https://er.educause.edu/articles/2015/7/taking-serious-games-seriously-in-education

DHS/FEMA (2025a), "National Level Exercise", https://www.fema.gov/emergency-managers/national-preparedness/exercises/national-level-exercise

DHS/FEMA (2025b), "Welcome to National Level Exercise 2020", https://www.preptoolkit.fema.gov/web/nle-2020

DHS/FEMA (2025c), "Exercise and Preparedness Tools", https://www.fema.gov/emergency-managers/national-preparedness/exercises/tools

Fox, Jacob (2024), "Top Cybersecurity Statistics for 2025", https://www.cobalt.io/blog/top-cybersecurity-statistics-2025

Guillen-Nieto, V, and Aleson-Carbonell M, (2012), "Serious games and learning effectiveness: The case of *"It's a Deal!"*, Computers & Education, 58 (23012) 435-448

Jacob, Johanna (2024), "Examining the Divide: Understanding Differential Reach and Accessibility in K-12 Cybersecurity Education", Ph.D. Dissertation, August, 2024, The University of Texas at San Antonio.

Kong, Yangtao, (2021), "The Role of Experiential Learning on Student's Motivation and Classroom Engagement", Frontiers in Psychology, 22 October 2021, doi: 10.3389/fpsyg.2021.771272

Learning Lands (accessed 2025), "The Benefits of Gaming in Education", https://learn.culturalinfusion.org.au/the-benefits-of-gaming-in-education/

Nachimuthu, K., and Vijayakumari, G. (2011), "Role of Educational Games Improves Meaningful Learning", *i-Manager's Journal of Educational Technology*, Vol. 8, No. 2, July-September 2011.

NIST (2024), "The NIST Cyber Security Framework (CSF) 2.0" https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Srėbaliūtė, Agnė. (2024), "Best practices on cybersecurity budget allocation: a research-based guide", h ttps://nordlayer.com/blog/best-practices-cybersecurity-budget-research-guide/